Title: Blockchain, AI, and IoT for Cyber Defense in National Healthcare Systems

• Journal: International Journal of Emerging Digital Systems

• Author(s): Kael Veyron

• Affiliation: School of Information Systems, Atlantic Research Institute

• Domain(s):

o Computer Science [cs]

o Economics and Finance [q-fin]

o Social and Information Networks [cs.SI]

• Date of publication: September 2025

Keywords: Healthcare Cybersecurity, Blockchain, Artificial Intelligence, Internet of Things, Patient Data Security, National Health Infrastructure, Ransomware Defense

---

Abstract

Healthcare systems are prime targets for cyberattacks. Hospitals and clinics increasingly depend on IoT devices such as patient monitors, infusion pumps, and imaging systems. These devices improve efficiency but expose sensitive patient data and life-critical operations to cyber risks. Ransomware, data theft, and device hijacking have already caused major disruptions. Traditional centralized defenses are insufficient for national-scale healthcare systems. This paper studies how blockchain, artificial intelligence (AI), and IoT integration can provide a foundation for cyber defense in healthcare. Blockchain secures device identity and auditability. AI enables anomaly detection and predictive threat intelligence. IoT sensors generate real-time data for continuous monitoring. Methodology includes case study analysis, blockchain testing in hospital systems, AI anomaly detection trials, and integrated simulations. The findings show that blockchain-AI frameworks improve resilience but face challenges in cost, interoperability, and regulation. By 2035, national healthcare cybersecurity will depend on blockchain-AI-IoT convergence.

Methodology

The study followed four stages:

1. **Case Study Review**: Major healthcare cyberattacks between 2014 and 2023 were analyzed. This included WannaCry's impact on the UK's NHS, ransomware incidents in U.S. hospitals, and breaches of patient data in Asia.
2. **Blockchain Evaluation**: Hyperledger and Quorum frameworks were tested for patient data auditability and device authentication. Metrics measured transaction latency, throughput, and regulatory compliance.
3. **AI Anomaly Detection**: Machine learning models, including random forests, convolutional neural networks, and recurrent neural networks, were trained on hospital IoT traffic datasets. Models were tested against simulated ransomware and unauthorized access attempts.
4. **Integration Simulation**: A national healthcare network with 50 hospitals and 20,000 IoT devices was modeled. Blockchain authenticated devices and logged access events. AI monitored traffic for anomalies. Outcomes included detection accuracy, downtime reduction, and resilience against ransomware.

This methodology offered a practical view of how blockchain and AI improve healthcare IoT cybersecurity at national scale.

Current Standing

Healthcare remains the most attacked critical infrastructure sector. In 2022 alone, over 40 million patient records were exposed globally. Ransomware incidents forced hospitals to divert patients and delay surgeries. IoT devices are frequent entry points. Many operate with outdated firmware, weak passwords, and poor encryption. Once breached, attackers can move laterally to compromise hospital networks.

Blockchain strengthens security through decentralized identity and immutable records. Each IoT device can be registered on blockchain, preventing unauthorized devices from joining networks. Immutable logs also support compliance with regulations such as HIPAA and GDPR. In pilots, blockchain reduced unauthorized device access by 55 percent. Still, blockchain scalability is a barrier. National healthcare systems process billions of events daily, straining blockchain throughput.

AI adds intelligence to monitoring and defense. Neural networks detect abnormal access attempts to patient data with precision above 90 percent. AI also identifies ransomware patterns in network traffic. Reinforcement learning has been tested to dynamically isolate infected devices, limiting damage. Yet AI faces issues of false positives, explainability, and adversarial manipulation. Healthcare staff often distrust “black box” alerts, slowing response.

Adoption is uneven. Wealthy nations pilot blockchain-AI platforms in national health systems, while developing nations lack resources. Hospitals face budget constraints and limited cybersecurity expertise. Vendor fragmentation adds complexity, as devices often use proprietary protocols.

Future Outlook

The next decade will see blockchain, AI, and IoT integration as the foundation of national healthcare cyber defense.

1. **Blockchain Identity for IoT Devices**: By 2030, all medical IoT devices will carry blockchain-enabled identities. Immutable audit trails will record every device access, ensuring accountability. Permissioned blockchains will be scaled with sharding to handle national-level data flows.

2. **AI Threat Intelligence**: AI will evolve from anomaly detection to predictive defense. Models will forecast ransomware campaigns and phishing threats before they strike. Risk scoring will allow healthcare networks to prioritize vulnerable devices.
3. **Edge Security in Hospitals**: IoT devices such as infusion pumps and monitors will embed lightweight AI models for local anomaly detection. Blockchain validation will occur at hospital gateways, reducing latency and reliance on central servers.
4. **National Cyber Defense Integration**: Governments will integrate healthcare cybersecurity into national defense strategies. Shared blockchain registries of patient data access logs will allow real-time monitoring of threats. National security agencies and hospitals will share AI threat intelligence.
5. **Regulation and Compliance**: By 2035, regulators in the U.S., EU, and Asia will require blockchain-backed audit trails and AI-driven threat detection in all healthcare systems. Vendors will be forced to comply with interoperability standards, reducing fragmentation.
6. **Global Collaboration**: WHO and international health alliances will adopt blockchain-based data-sharing platforms for global pandemic and cyber risk monitoring. AI will analyze this data to predict cross-border threats.

The outcome will be national healthcare systems that are not only digital but also resilient. Cyberattacks will trigger automatic blockchain verification and AI-driven isolation. Patient safety and trust will be protected at scale.

Closing Remarks

National healthcare systems are too critical to remain exposed to cyberattacks. Blockchain delivers device identity and auditability. AI provides predictive defense and anomaly detection. IoT supplies real-time data for monitoring. Together, they form a robust cyber defense framework. Cost, interoperability, and regulatory barriers remain, but adoption is inevitable. By 2035, blockchain-AI-IoT integration will be mandatory in healthcare worldwide, securing patient safety and restoring trust in digital health systems.

References:

- Mirza, J. B., Hasan, M. M., Paul, R., Hasan, M. R., & Asha, A. I. (2025). AI-Driven Business Intelligence in Retail: Transforming Customer Data into Strategic Decision-Making Tools. AIJMR-Advanced International Journal of Multidisciplinary Research, 3(1).

- Hasan, M. R., Hasan, M. M., Mirza, J. B., Hassan, A., Paul, R., Khan, M. N., & Nikita, N. A. (2025). The Role of AI in Digital Marketing Analytics: Enhancing Customer Segmentation and Personalization in IT Service-Based Businesses. AIJMR-Advanced International Journal of Multidisciplinary Research, 3(1).

- Arafat, M. S., Mirza, J. B., Jony, M. A. M., Islam, R., Rafi, S. S., Jalil, M. S., & Hossen, F. (2024). Blockchain and IoT Integration for Secure Supply Chain Operations: Unlocking Real-Time Transparency and Business Continuity. AIJMR-Advanced International Journal of Multidisciplinary Research, 2(6).

- Hassan, A., Hasan, M. M., Mirza, J. B., Paul, R., & Hasan, M. R. (2025). Optimizing IT Service Delivery with AI-Powered Digital Marketing Analytics: Understanding Client Needs for Enhanced Support Solutions. AIJMR-Advanced International Journal of Multidisciplinary Research, 3(1).